Changement de comportement de la clé GETVPN KEY Rekey

Contenu

Introduction

Ce document décrit les changements de comportement de la clé de chiffrement de clé GETVPN (KEK). Il inclut Cisco IOS® version 15.2(1)T et Cisco IOS-XE 3.5 version 15.2(1)S). Ce document explique ce changement de comportement et les problèmes potentiels d'interopérabilité qui en découlent.

Contribution de Wen Zhang, ingénieur TAC Cisco.

Ancien comportement

Avant la version 15.2(1)T de Cisco IOS, la clé KEK est envoyée par le serveur de clés (KS) lorsque la clé actuelle expire. Le membre du groupe (GM) ne tient pas de compteur pour suivre la durée de vie restante de la clé. La clé courante est remplacée par une nouvelle clé uniquement lorsqu'une nouvelle clé KEK est reçue. Si le Mécanisme mondial ne reçoit pas de clé KEK à l'expiration prévue de la clé KEK, il ne déclenche pas une nouvelle inscription au KS, et il conserve la clé existante sans la laisser expirer. Cela peut entraîner l'utilisation de la clé après sa durée de vie configurée. En outre, comme effet secondaire, il n'y a aucune commande sur le GM qui indique la durée de vie de KEK restante.

Nouveau comportement

Le nouveau comportement de la clé KEK comprend deux modifications :

- Sur le KS - les clés KEK sont envoyées avant l'expiration du KEK en cours, comme une clé REK (Traffic Exchange Key).
- Sur le GM - Le GM maintient un compteur pour suivre la durée de vie de la clé restante et

déclenche une nouvelle inscription si la clé KEK n'est pas reçue.

Comportement nouveau de KS

Avec le nouveau comportement de la clé, le KS démarre une clé KEK avant l'expiration de la clé courante selon cette formule.

$$KEK\_rekey\_time = KEK\_lifetime - (200 + (\#\_of\_retran * retran\_interval) + (5 * (1 + \frac{\#\_of\_registered\_GMs}{50})))$$

Note: Dans le calcul ci-dessus, la partie en surbrillance rouge est utilisée uniquement avec une clé de rediffusion unicast.

En fonction de ce comportement, un KS commence à reculer une clé au moins 200 secondes avant l'expiration de la clé courante. Une fois la nouvelle clé envoyée, le KS commence à utiliser la nouvelle clé pour toutes les clés TEK/KEK suivantes.

GM Nouveau comportement

Le nouveau comportement de la GM comprend deux changements :

1. Il applique une expiration de durée de vie KEK en ajoutant un minuteur pour suivre la durée de vie de KEK restante. Lorsque ce compteur expire, la clé KEK est supprimée sur le GM et un nouvel enregistrement est déclenché.
2. Le GM s'attend à ce qu'une nouvelle clé KEK se produise au moins 200 secondes avant l'expiration de la clé actuelle (voir changement de comportement KS). Un autre minuteur est ajouté de sorte que, dans le cas où la nouvelle clé n'est pas reçue au moins 200 secondes avant l'expiration de la clé actuelle, la clé est supprimée et une nouvelle inscription est déclenchée. Cet événement de suppression et de réenregistrement KEK se produit dans l'intervalle de temporisation de (expiration KEK - 190 secondes, expiration KEK - 40 secondes).

En plus des modifications fonctionnelles, les sorties de la commande **show** GM sont également modifiées pour afficher la durée de vie restante de KEK en conséquence.

```
GM#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 10.1.11.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
```

```
Registration status : Registered
Registered with : 10.1.11.2
Reregisters in : 81 sec     <=== Reregistration due to TEK or
KEK, whichever comes first
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Acks sents : 0

ACL Downloaded From KS 10.1.11.2:
access-list deny ospf any any
access-list deny eigrp any any
access-list deny udp any port = 848 any port = 848
access-list deny icmp any any
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 56     <=== Running timer for remaining KEK
lifetime
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0xD835DB99(3627408281)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (2228)
Anti-Replay(Time Based) : 10 sec interval
```

Problèmes d'interopérabilité

Avec ce changement de comportement de la clé KEK, le problème d'interopérabilité du code doit être pris en compte lorsque KS et GM ne peuvent pas exécuter les deux versions d'IOS qui ont ce changement.

Dans le cas où le GM exécute l'ancien code et le KS exécute le nouveau code, le KS envoie la clé KEK avant l'expiration du code KEK, mais il n'y a pas d'autre impact fonctionnel notable. Toutefois, si un GM exécutant le nouveau code s'enregistre auprès d'un KS exécutant l'ancien code, le GM peut faire l'objet de deux enregistrements de domaine d'interprétation de groupe (GDOI) afin de recevoir le nouveau cycle de clé KEK par clé KEK. Une séquence d'événements se produit lorsque ceci se produit :

1. L'enregistrement GM avant l'expiration de la clé actuelle, puisque la clé KS n'enverra la clé

KEK que lorsque la clé actuelle expire. Le module GM reçoit la clé KEK, et elle est la même que celle qu'il possède actuellement, avec une durée de vie inférieure à 190 secondes restante. Ceci indique au GM qu'il est enregistré avec un KS sans changement de clé KEK.

```
%GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may
have expired/been cleared, or didn't go through. Re-register to KS. %CRYPTO-5-GM_REGSTER:
Start registration to KS 10.1.11.2 for
group G1 using address 10.1.13.2 %GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to
Unicast Rekey. %GDOI-5-SA_KEK_UPDATED: SA KEK was updated %GDOI-5-SA_TEK_UPDATED: SA TEK
was updated %GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.11.2 complete
for group G1 using address 10.1.13.2 %GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS:
Installation of
Reg/Rekey policies from KS 10.1.11.2 for group G1 & gm identity 10.1.13.2
```

2. Le GM supprime la KEK à son expiration à vie et définit un compteur d'enregistrement de (expiration de la KEK, expiration de la KEK + 80).

```
%GDOI-5-GM_DELETE_EXPIRED_KEK: KEK expired for group G1 and was deleted
```

3. ÀI'expiration du délai d'enregistrement, le GM se réenregistre et recevra la nouvelle clé KEK.

```
%GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may
   have expired/been cleared, or didn't go through. Re-register to KS.
%CRYPTO-5-GM_REGSTER: Start registration to KS 10.1.11.2 for
group G1 using address 10.1.13.2 %GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to
Unicast Rekey. %GDOI-5-SA_KEK_UPDATED: SA KEK was updated %GDOI-5-SA_TEK_UPDATED: SA TEK
was updated %GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.11.2 complete for
group G1 using address 10.1.13.2 %GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation
of
Reg/Rekey policies from KS 10.1.11.2 for group G1 & gm identity
10.1.13.2
```

Recommandations

Dans un déploiement GETVPN, si l'un des codes GM Cisco IOS a été mis à niveau vers l'une des versions avec le nouveau comportement de clé KEK, Cisco recommande que le code KS soit également mis à niveau afin d'éviter le problème d'interopérabilité.